NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

OPERATIONAL BENEFIT OF IMPLEMENTING VoIP IN A TACTICAL ENVIRONMENT

by

Rosemary Lewis

June 2003

Thesis Advisor:	Dan C. Boger
Second Reader:	Rex Buddenberg

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Operational Benefit of Implementing VoIp in a Tactical Environment			**5. FUNDING NUMBERS**
6. AUTHOR(S) Rosemary Lewis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement (mix case letters)			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

In this thesis, Voice over Internet Protocol (VoIP) technology will be explored and a recommendation of the operational benefit of VoIP will be provided. A network model will be used to demonstrate improvement of voice End-to-End delay by implementing quality of service (QoS) controls. An overview of VoIP requirements will be covered and recommended standards will be reviewed. A clear definition of a Battle Group will be presented and an overview of current analog RF voice technology will be explained. A comparison of RF voice technology and VoIP will modeled using OPNET Modeler 9.0.

14. SUBJECT TERMS Voice Over Internet Protocol, VoIP, ADNS, Quality of Service, QoS			**15. NUMBER OF PAGES** 78
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OPERATIONAL BENEFIT OF IMPLEMENTING VoIP IN A TACTICAL ENVIRONMENT

Rosemary Lewis
Lieutenant, United States Navy
B.S., Troy State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author: Rosemary Lewis

Approved by: Dan C. Boger
Thesis Advisor

Rex A. Buddenburg
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, Voice over Internet Protocol (VoIP) technology will be explored and a recommendation of the operational benefit of VoIP will be provided. A network model will be used to demonstrate improvement of voice End-to-End delay by implementing quality of service (QoS) controls. An overview of VoIP requirements will be covered and recommended standards will be reviewed. A clear definition of a Battle Group will be presented and an overview of current analog RF voice technology will be explained. A comparison of RF voice technology and VoIP will modeled using OPNET Modeler 9.0.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to thank Professor Dan Boger and Professor Rex Buddenberg for their advice and patience during my research process. I would also like to thank the following students for their help and assistance through out this project: LT Pete Laird and LT JaJa Marshall. I would like to give a special thanks to my family and all of my friends, without their love and support this achievement would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. VOIP

A. INTRODUCTION

This thesis investigates the operational feasibility of implementing voice over IP technology to enhance the U.S. Navy voice communications. This report will examine the convergence of data and voice packets being exchanged over the Local Area Network (LAN) verse the current configuration of data and voice packets being exchanged over Radio Frequency (RF) analog pipelines.

B. PURPOSE

The benefit of this research is to determine if VoIP technology will enhance the U.S. military's communications in a tactical environment. Some of the key considerations will be bandwidth and QoS issues. This research will present a comprehensive overview of how the U.S. military communicates today and will compare that communication technology with VoIP technology. In addition, this study will identify possible problems with VoIP technology such as security and time delays and suggest some alternatives to those problems.

C. DISCUSSION

The World Wide Web (WWW) and the Internet have grown exponentially since their inception and represent a revolutionary and potentially effective communication medium. Today, most of the U.S. voice communications are transmitted via satellite communications and that are not associated with the Internet. The VoIP technology offers an enhanced process of voice transmissions of vital information creating a virtual communication environment. VoIP is defined as:

> A process that transports speech signals in an acceptable way from sender to destination over an IP network. [Ref 1]

Thus, this research centers on VoIP technology as an enhanced form of communication, particularly in tactical Military Operations. Some points of consideration will be bandwidth and latency.

D. SCOPE OF THESIS

The scope of this thesis will include: (1) A brief overview of existing U.S. military communications architecture, (2) Define the essential elements of VoIP

technology, (3) Use OPNET to build a network model of a Battle Group and evaluate the network latency by employing QoS controls, (4) Weigh the benefits of integrating VoIP technology in the U.S. military existing communication structure.

E. METHODOLOGY

- Literature Review. Conduct a literature search of books, journal articles, previous research and other library information resources.
- Statistical Analysis. Conduct a review of empirical data collected from OPNET Modeler network model of a Battle Group designed to analyze latency in the network.
- Results. The results of the analysis and review are synthesized and crafted into a coherent plan for employment of VoIP technology in support of tactical Military Communications

II. VOICE OVER INTERNET PROTOCOL

A. INTRODUCTION

Technology has been advancing exponentially since the advent of the Internet. New forms of communications have made possible the sharing of ideas and information that has launched the world into a new digital age possible. Organizations around the world are now searching for the next step in the communications boom that can tie all of the existing media together into a system enabling face-to-face virtual interaction. Recent innovations in the Voice-over Internet Protocol (VoIP) field have are quickly approaching the final barriers restraining the full integration of current communications systems.

B. VOICE OVER INTERNET PROTOCOL OVERVIEW

VoIP technology has been developed to condense telephone voice data and transfer it along the signaling data lines now present for Internet and Intranet communication. These advances aspire to considerably reduce the amount of hardware and physical space needed to support available technology and the supervision necessary to maintain both networks.

Perhaps the one of the greatest advantages of an IP system is its capacity to unify a battle group's communications system in ways that are unachievable with analog voice RF technology. An IP system can seamlessly integrate all forms of battle group communication, making any information available to any battle group ship in the unit battle group at any time.

1. Functions Made Available by IP Technology

- The convergence of voice mail and email into one multimedia system, accessible from remote phone, shipboard phone (analog/digital) or PC.
- Multi-media video conferencing delivered to any endpoint in a battle group.
- Remote location access to all of the physical and data resources of a battle group.

C. VOICE OVER INTERNET PROTOCOL PROCESS

In every Internet/Intranet digital data network there is a vast amount of bandwidth that goes unused. VoIP technology capitalizes on this dormant bandwidth, using it to transmit voice data along with the signaling data. When a call is placed using a VoIP system, standard telephone voice data is passed to an IP platform where it is encoded into packets. Once compressed, these packets are transmitted to the signaling data network (LAN, WAN), which carries the connection for digital communication. From the Data line, these packets are capable of traversing any network including Internet, Asynchronous Transfer Mode (ATM), Frame Relay, and satellite. By implementing an IP solution, a battle group's communication network can be enhanced significantly.

D. VOICE OVER INTERNET PROTOCOL CONSIDERATIONS

VoIP technology, as with all telecommunications technology, is governed by sets of standards that have been established by the International Telecommunications Union (ITU-T). For an IP solution to be successful it must communicate following ITU specified protocols that dictate the requirements for audio and video transmissions over the Internet. For VoIP the following standards are the most commonly supported protocol:

1. H.323 Standard

- H.323 is the most widely supported protocol. The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed Quality of Service (QoS). These networks dominate today's corporate desktops and include packet-switched TCP/IP and IPX over Ethernet, Fast Ethernet and Token Ring network technologies. Therefore, the H.323 standards are important building blocks for a broad new range of collaborative, LAN-based applications for multimedia communications. [Ref 2]

2. Session Initiation Protocol (SIP) Standard

- The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. These multimedia sessions include multimedia conferences, distance learning, Internet telephony and similar applications. SIP can invite both persons and "robots", such as a media storage service. SIP can

invite parties to both unicast and multicast sessions; the initiator does not necessarily have to be a member of the session to which it is inviting. Media and participants can be added to an existing session. [Ref 2]

- SIP can be used to initiate sessions as well as invite members to sessions that have been advertised and established by other means. Sessions can be advertised using multicast protocols such as SAP, electronic mail, news groups, web pages or directories (LDAP), among others. [Ref 2]
- SIP transparently supports name mapping and redirection services, allowing the implementation of ISDN and Intelligent Network telephony subscriber services. These facilities also enable personal mobility. In the parlance of telecommunications intelligent network services, this is defined as: "Personal mobility is the ability of end users to originate and receive calls and access subscribed telecommunication services on any terminal in any location, and the ability of the network to identify end users as they move. Personal mobility is based on the use of a unique personal identity (i.e., personal number)." [1]. Personal mobility complements terminal mobility, i.e., the ability to maintain communications when moving a single end system from one subnet to another. [Ref 2]
- SIP supports five facets of establishing and terminating multimedia communications. [Ref 2]
- User location: determination of the end system to be used for communication. [Ref 2]
- User capabilities: determination of the media and media parameters to be used. [Ref 2]
- User availability: determination of the willingness of the called party to engage in communications. [Ref 2]
- Call setup: "ringing", establishment of call parameters at both called and calling party. [Ref 2]

3. Media Gateway Control Protocol (MGCP) Standard

- The Media Gateway Control Protocol (MGCP) standard MGCP Basics The Media Gateway Control Protocol, or MGCP, was designed to address the requirements of production IP telephony networks that are built using? Decomposed? VoIP gateways. MGCP based VoIP solutions separate call control (signaling) intelligence and media handling. MGCP functions as an internal protocol between the separate components of a decomposed MGCP compliant VoIP gateway. More specifically, MGCP is a protocol used by external call control elements called Media Gateway Controllers (MGCs) to control Media Gateways (MGs). Decomposed MGCP-compliant VoIP gateways appear to the outside as a single VoIP gateway. [Ref 2]

- Examples of VoIP gateways include:
  - Trunking gateways that interface the circuit switched telephony network to VoIP networks
  - Residential gateways that provide traditional analog (RJ11) interfaces to VoIP networks
  - Access gateways that provide traditional analog (RJ11) or digital PBX interfaces to VoIP networks
  - IVR Announcement Servers that can provide interactive voice response and announcements to VoIP networks

4. H.324 Standard

- H.324 addresses and specifies a common method for sharing video, data, and voice simultaneously using V.34 modem connections over a single analog Plain Old Telephone System (POTS) telephone line. It also specifies interoperability under these conditions, so that videophones, for example, based on H.324 will be able to connect and conduct a multimedia session. [Ref 2]

5. H.320 Standard

- H.320 is a standard used in visual telecommunications to ensure compatibility amongst terminals produced by different vendors. H.320 is known as an "umbrella" standard. This means it specifies certain protocols for video, audio, control, etc. There are various classes of H.320 that support a variety number of protocols. However, there are mandatory requirements that ensure all H.320 compatible systems can communicate with one another. There are also optional requirements that can allow systems to provide additional functionality. It should be noted that, though, that this functionality is sacrificed for compatibility when communicating with systems that only meet the minimal requirements for H.320. [Ref 2]

The above standards representing a common ground between systems, making IP systems compatible with existing systems for conference calling, video conferencing, and virtual meeting applications.

One major contention that has been placed against VoIP technology is Quality of Service (QoS).

6. Voice Over Internet Protocol QoS

QoS is made up of bandwidth efficiency, interactivity, latency, jitter and packet loss. Anytime you implement QoS you trade off at least one of these characteristics to optimize another.

As technology advanced, sound quality has improved but some issues remain inherent to the packetizing procedure (Packet Loss), jitter and delay being the most prevalent.

- Packet loss is the term used to describe data packets that do not arrive at the intended destination. Packets contain the information of the conversation. If IP packets are lost, parts of the conversations will break up.
- Jitter refers to a voice data problem that occurs because of systems varying allotment of times allowed between packets. To compensate, a receiving system has to wait for all of the transmission packets to arrive before playing them, which results in delay. [Ref 3]
- Latency is the time it takes for a call to travel from the originating telephone to the termination telephone. Unless this time is under about 300 milliseconds roundtrip, call quality will be inferior to the regular telephone network. [Ref 3]
- Delay is the result of a number of contributing factors including jitter, but is primarily caused by an improper amount of bandwidth available in a system. In a large, high-volume application, voice data packets can run into interference and experience delay as a result of high traffic patterns. To counteract the delay problem, different voice coding systems have been introduced to change the size of data packets and increase the amount of compression; minimizing the quantity of bandwidth needed to transport voice data. [Ref 3]

THIS PAGE INTENTIONALLY LEFT BLANK

III. CARRIER BATTLE GROUP

A. INTRODUCTION

The exact make-up of a Carrier Battle Group has varied since the end of the Cold War but its mission has remained constant to gain and maintain battlespace dominance so it can project power. First, it is important to note that there really is no real definition of a battle group. Task groups are formed and disestablished on an as-needed basis, and one may be different from another. However, they all are comprised of similar types of ships. While most ships today are multi-mission platforms, their primary missions can be considered as follows::

- **Carrier** – The carrier provides a wide range of options to the U.S. government from simply showing the flag to attacks on airborne, afloat and ashore targets. The carrier, through its air wing, is the primary power projector by conducting strike warfare. The air wing retains considerable anti-air, anti-surface, and anti-submarine capabilities as well. These ships also engage in sustained operations in support of other forces. [Ref 4] Included in the communications suite are the following unlimited Dual DAMA, Challenge Athena, SHF, EHF, UHF, HF, and VHF.
- **Two Guided Missile Cruisers** – multi-mission surface combatants. Equipped with *Tomahawks* for long-range strike capability. Guided missile cruisers are concerned with anti-air warfare and have a growing capability for theater ballistic missile defense that extends throughout the battlespace. [Ref 4] Included in the communications suite are the following SHF, dual DAMA, VHF, HF, UHF, and dual INMARSAT HSD.
- **Guided Missile Destroyer** – multi-mission surface combatant, used primarily for anti-air warfare (AAW). [Ref 4] Included in the communications suite are the following dual DAMA 5kHz, HF, UHF, and VHF.
- **Destroyer** – primarily for anti-submarine warfare (ASW). Destroyers are generally used to screen the carrier from surface and undersea threats, however they also share in the anti-air warfare role and strike missions. [Ref 4] Included in the communications suite are the following HF, UHF, VHF, and single DAMA.
- **Frigate** – primarily for anti-submarine warfare (ASW). Frigates are generally used to screen the carrier from surface and undersea threats, however they also share in the anti-air warfare role and strike missions. [Ref 4] Included in the communications suite are the following HF, UHF, VHF, and single DAMA.

- **Two Attack Submarines** – in a direct support role seeking out and destroying hostile surface ships and submarines Attack submarines protect the carrier against surface and undersea threats, and also provide national intelligence and tactical intelligence to the battlegroup. Submarines also provide strike capabilities with their tomahawk missiles. [Ref 4] Included in the communications suite are the following EHF, HF, and UHF.
- **Combined Ammunition, Oiler, and Supply Ship** – provides logistic support enabling the Navy's forward presence: on station, ready to respond, Logistics ships, like the Fast Combat Support Ship, keep the the battle group topped off with fuel, ammo, parts, and food. [Ref 4] Included in the communications suite are the following HF, UHF, VHF and single DAMA.

The Carrier Battle Group (CVBG) could be employed in a variety of roles, all of which would involve the gaining and maintaining of battle space dominance. Communications is definitely a vital role in the mission of a battle group.

B. VOICE COMMUNICATIONS INFRASTRUCTURE

Communications is the cornerstone to today's military forces. Without effective communications the navy is limited to the capabilities within the lifelines of the ship. New doctrine is being implemented to use Network Centric Warfare (NCW) as the force multiplier of the future. The navy currently uses satellite and line of sight (LOS) communications utilizing the Radio Communications System (RCS) to conduct Network Centric operations. The RCS consists of several exterior communications subsystems, which in combination provide all exterior communications requirements for the battle group with the exception of the Special Intelligence Communications requirements. The RCS subsystems are turnkey installations and consist of the following subsystems: High Frequency Communications System, Very High Frequency Communications (VHF Comms) System, Ultra High Frequency Line-of-Sight Communications (UHF LOS Comms) System, Ultra High Frequency Satellite Communications (UHF SATCOM) System, Extremely High Frequency Satellite Communications (EHF SATCOM) System, Super High Frequency Satellite Communications (SHF SATCOM) System, Communications Support Segment (CSS), Naval Modular Automated Communications System (NAVMACS) II, and the Bridge To Bridge Communications (BTB Comms) System. The following is a brief description of the various communications systems typically used in a battle group.

The High Frequency Radio Group provides remotely controlled, rapidly tunable, reliable Ship-to-Ship and Ship to shore communications.

- The **High Frequency Communications System** consists of the High Frequency Radio Group (HFRG) is a fully automated subsystem of the external RCS aboard surface ships. The HFRG operates in the Very Low Frequency (VLF), Low Frequency (LF), Medium Frequency (MF) and High Frequency (HF) frequency bands and supports full duplex, half duplex and simplex operation for tactical and long-haul voice, interrupted continuous-wave, teletype and digital data communications in the Lower Sideband (LSB), Upper Sideband (USB), Independent Sideband (ISB), Amplitude Modulation Equivalent (AME) and Link 11 modes of operation. The HFRG consists of three subsystems: the transmit subsystem, the receive subsystem and the control/monitor subsystem (CMS). [Ref 5]

The VHF Comms System primarily supports line-of-sight (LOS) communications between accomplishing units and is comprised of several different Radio Groups or subsystems

- The **Very High Frequency Communications (VHF Comms) System** is utilized to transmit and receive tactical, operational and administrative information (both voice and data) in the VHF range (30-300 MHz). Most of the Radio Groups are functionally interchangeable and therefore are not individually dedicated to a specific circuit or function. [Ref 5]

The Ultra High Frequency Line-of-Sight Communications (UHF LOS Comms) is utilized to transmit and receive tactical, operational and administrative information (both voice and data) in the UHF range (300 MHz - 3 GHz).

- The UHF LOS Comms System is capable of operating in either the UHF LOS or UHF Satellite Communications (UHF SATCOM) mode. Most of the UHF LOS equipments are functionally interchangeable and therefore are not individually dedicated to a specific circuit or function. [Ref 5]
- The **Ultra High Frequency Satellite Communications (UHF SATCOM) System** provides communication links, via satellite, between designated mobile units and shore sites worldwide. The UHF SATCOM system is one of three SATCOM systems installed and operates in the UHF range. The SATCOM systems, combined, represent a composite of information exchange systems that use the satellites as relays for communications and control as well as quality monitoring subsystems that provide data to manage satellite resources. The shipboard SATCOM configurations vary in size and complexity and are dependent upon the message traffic level, types of communications and operational missions of the ship. The UHF SATCOM system provides multichannel satellite transmission and reception and is comprised of two distinct, but related,

subsystems: (1) UHF SATCOM receiving set and (2) UHF SATCOM transceivers and UHF Demand Assigned Multiple Access (DAMA) equipment. [Ref 5]

- The **UHF SATCOM receiving set** is the UHF component of the High Speed Fleet Broadcast (HSFB) and is used to receive the downlink Fleet Broadcast signal and demultiplex it into the different Fleet Broadcast baseband circuits. [Ref 5]
- The **Extremely High Frequency Satellite Communications (EHF SATCOM) System** provides communication links, via satellite, between designated mobile units and shore sites worldwide. The EHF SATCOM system is one of three SATCOM systems and operates in the EHF range (30-300 GHz). The SATCOM systems, combined, represent a composite of information exchange systems that use the satellites as relays for communications and control as well as quality monitoring systems that provide data to manage satellite resources. The shipboard SATCOM configurations vary in size and complexity and are dependent upon the message traffic level, types of communications and operational missions of the ship. The EHF SATCOM system is a general purpose satellite communications terminal that provides survivable, jam-resistant, low probability of intercept communications for secure voice, teleprinter and data circuits. The system provides four primary transmit/receive channels, four secondary transmit/receive channels and four receive only channels. [Ref 5]
- The **Super High Frequency Satellite Communications (SHF SATCOM) System** provides communication links, via satellite, between designated mobile units and shore sites worldwide. The SHF SATCOM system is one of three SATCOM systems installed and operates in the SHF range (3-30 GHz). The SATCOM systems, combined, represent a composite of information exchange systems that use the satellites as relays for communications and control as well as quality monitoring subsystems that provide data to manage satellite resources. The shipboard SATCOM configurations vary in size and complexity and are dependent upon the message traffic level, types of communications and operational missions of the ship. The SHF SATCOM system provides highly reliable, high capacity, long range ship to shore communications with a high degree of immunity to jamming and direction finding. [Ref 5]

The Bridge to Bridge Communications System is used primarily for communications between bridge personnel aboard surface units operating in close proximity to each other such as during underway replenishment.

- The **Bridge To Bridge Communications System** is a stand-alone, Very High Frequency (VHF), radio system comprised of a Transceiver, handset, speakers and a dedicated antenna which provides the capability for short-range, nonsecure, voice communications in the VHF range. [Ref 5]

C. LAN/DATA COMMUNICATIONS INFRASTRUCTURE

Telecommunications used by US Naval Battle Group continues to migrate toward Internet Protocol (IP) based technology. Information Technology for the 21st Century (IT-21) focuses on modernizing local area networks (LAN) afloat and LANs or wide area networks (WAN) ashore (WAN).

IT-21 configured ships use SATCOM to communicate information with other ships or shore stations not in LOS of each other. Shipboard C4I systems use SATCOM as their access point to these networks. As information demand increases, so does the value of the bandwidth on the SHF SATCOM. A solution to this growing problem could be the implementation of VoIP technology.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. IMPLEMENTING VOIP

A. INTRODUCTION

The implementation of Voice over IP technology in a Battle Group would definitely enhance tactical voice communications. Analog RF voice communications has been around for decades and has is proven to be a reliable means of transmitting and receiving voice transmissions.

1. Analog RF Voice Communications

Analog RF voice communications is the primary means of communications in the Battle Group. There are some advantages of RF which include:

- Short range & tactical communication
- Provide direct communications with other ships
- Minimum delay
- Instant acknowledgement
- Line of sight characteristics- reduces the chance of enemy interception

Disadvantages of RF include:

- Susceptible to static, enemy interference or high local noise level
- Wave propagation unpredictable i.e. tactical transmission may be heard from great distance.

2. VOIP Advantages

When fully implemented, VoIP will significantly improve the way a Battle group communicates and operates in a tactical environment. At the Battle group level, the benefits include:

- Improved interoperability by using a common IP infrastructure.
- Improved ability to conduct collaborative planning by using features like multicasting, which allows the voice transmission to be broadcasted to every ship in the Battle group and also allows for each ship to respond to all ships via the same medium.
- Improved bandwidth management because it allows voice communications to be transmitted over the IP network. This reduces the demand on RF circuits and those resources are available for other purposes.
- Overall VoIP provides the Navy with another tool that enhances Battle group communication in a tactical environment.

3. VOIP Baseline

One of the first steps in the implementation process is to determine the VOIP Baseline.

Four primary components:

- Infrastructure

  The infrastructure can support multiple client types such as hardware phones, software phones, and video devices. Typical products used to build an infrastructure include voice gateways (non-routing, routing, and integrated), switches, Voice application systems

- IP Phones

  IP Phones are a full range of intelligent communication devices designed to take advantage of the power of your data network, while providing the convenience and ease-of-use you have come to expect from a phone. In the IP environment, each phone has an Ethernet connection. IP phones provide the functionality you expect to receive from a traditional telephone, as well as more complicated features, such as the ability to access World Wide Web sites.

- Call Manager

  At the heart of the IP telephony system is the Call Manager, the software-based call processing agent. Call Manager software extends telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.

- Voice Software

  Voice applications are physically independent from the call processing and voice processing infrastructure, and they may reside anywhere within the network. Leveraging a single network infrastructure, provides an open platform for powerful productivity applications, and serves as a solid foundation for future convergence-based applications that will continue to advance communications

4. SHIPBOARD Baseline

The primary media for voice communications in a Battle group is an RF transmission. DoN installations employ Automated Digital Network System (ADNS) as their network backbone. ADNS uses commercial off the shelf (COTS) protocols, processors and routers to create a robust and flexible networking environment. ADNS provides an interface to all RF media from HF to EHF and provides the total throughput for access needed. Dynamic allocation of bandwidth usage on a common IP

infrastructure ultimately leads to more efficient use of available bandwidth. Efficiencies of common infrastructure are especially critical in the bandwidth choke point of ship to shore communication links.

B. CONSIDERATIONS

1. Scalability

The ability of a computer application or product to continue to function well as it is changed in size or volume in order to meet a user need. Typically, the rescaling is to a larger size or volume. The Battle Group must have the ability not only to function well in the rescaled situation, but to be able to take full advantage of it.

2. Interoperability

The ability of the systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

3. Reliability

Reliability is defined as an attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications. Similarly, reliable communication is, Communication where messages are guaranteed to reach their destination complete and uncorrupted and in the order they were sent. The Battle Group tactical voice communications system requires that the system is available at all times. Reliability and redundancy must be built into the system. The system must be designed to eliminate any single point of failure. The network supporting the VoIP technology must be fault tolerant, providing a robust voice communications system. VoIP technology must meet or exceed the current reliability standards of RF communications to be a viable solution.

4. Bandwidth Usage Packet Switching vs Circuit Switching

- Packet switching refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Packet switching, which is used in VoIP

technology, is more efficient in bandwidth usage but there is some amount of delay encountered.

- Circuit switching sometimes known as a connection-oriented network is a type of communications in which a dedicated channel is established for the duration of a transmission. A good example would be a T1 connect and this is the least efficient means of bandwidth usage.

5. Quality of Service Considerations

- Packet loss is a common occurrence in data networks, but computers and applications are designed to simply request a retransmission of lost packets. Dropped voice packets, on the other hand, are discarded, not retransmitted. Voice traffic can tolerate less than a 3 percent loss of packets (1% is optimum) before callers experience disconcerting gaps in conversation.
- Latency as a delay-sensitive application, voice cannot tolerate too much delay. Latency is the average travel time it takes for a packet to reach its destination. If there is too much traffic on the line, or if a voice packet gets stuck behind a large data packet (such as an email attachment), the voice packet will be delayed to the point that the quality of the call is compromised. The maximum amount of latency that a voice call can tolerate one way is 150 milliseconds (100 milliseconds is optimum).
- Jitter- In order for voice to be intelligible, consecutive voice packets must arrive at regular intervals. Jitter describes the degree of variability in packet arrivals, which can be caused by bursts of data traffic or just too much traffic on the line. Voice packets can tolerate about only about 75 milliseconds (40 milliseconds is optimum) of jitter delay.

6. Quality of Service Controls

QoS is the key to making voice-data networks a practical reality. Jitter, packet loss and excessive delay can wreak havoc on call quality. QoS mechanisms are available to properly control the factors of latency, jitter and packet loss to guarantee that VoIP delivers the same quality voice that users are accustomed to from dedicated voice networks.

To compensate for jitter, some VoIP equipment manufacturers provide jitter buffers in gateways or handsets. The key to minimizing jitter for voice traffic is to deploy a QoS mechanism capable of automatically detecting the required interval between packets, and adjusting queuing parameters in real time to ensure that this interval is maintained.

To deal with packet loss, some VoIP equipment manufacturers offer a repairing algorithm called silence insertion, which makes up for packet loss by inserting silence packets meant to emulate pauses in human speech. However, silence insertion and other such repairing algorithms do not prevent packet loss, but instead attempt to minimize the problem after the fact this is mere damage control, not proactive QoS. Therefore, it is also critical to deploy a QoS mechanism capable of preventing the conditions that lead to packet loss in the first place.

One of the most effective ways to minimize delay for voice traffic is to deploy a QoS solution capable of controlling the size of packets generated by data applications such as e-mail. Another highly effective way of minimizing delay is to deploy a QoS solution capable of capping queuing delay at a specified level, and discarding any packets that do not fit within this amount of delay. This will introduce a transitory blip in the voice call, but this is preferable to degrading the call from the time the congestion occurred.

THIS PAGE INTENTIONALLY LEFT BLANK

V. OPNET MODELER 9.0

A. OPNET CAPABILITIES

The OPNET simulation software has the ability to build hierarchical network models and manage complex network topologies with unlimited sub-network nesting. It can model wireless, point-to-point and multipoint links. This is the portion of the software that makes it a good tool for modeling a battle group's interaction.

OPNET can incorporate physical layer characteristics, environmental effects, account for delays, availability, and throughput characteristics of links. OPNET is a unique modeling tool because it has the ability to use geographical and mobility modeling by controlling each node's position dynamically or through predefined trajectories. Maps and other background graphics can be added to facilitate graphical representation for easier assimilation of data.

Results from OPNET are easily interpreted with comprehensive tools to display, plot and analyze time series, histograms, probability functions, parametric curves, and confidence intervals, which can be exported to spreadsheet form.

B. MODEL IMPLEMENTATION

This chapter will present a model that possesses characteristics necessary to evaluate the effects of quality of service (QoS) tools on a network transmitting voice packets. The model is a baseline scenario obtained from the OPNET tutorial with a few modifications to simulate network traffic of a battle group.

The architecture of the model chosen is related to a LAN communication network resembling that of a SIPRNET LAN of a Battle Group. Documentation for this model can be viewed in the OPNET project section of OPNET Modeler titled as QoS_Data_Voice and in appendix A of this report. An individual's own understanding of the subject and OPNET are required in order to investigate the performance and parameters input into the model.

C. MODEL DESCRIPTION

The figure below illustrates a Battle Group consisting of six ships of various types. Each ship in the Battle Group is passing voice packets over a SIPRNET LAN.

The model shown below in Figure 1 is a modification of OPNET Modeler 9.0 project titled QoS_Data_Voice. Details of this project are in Appendix A.

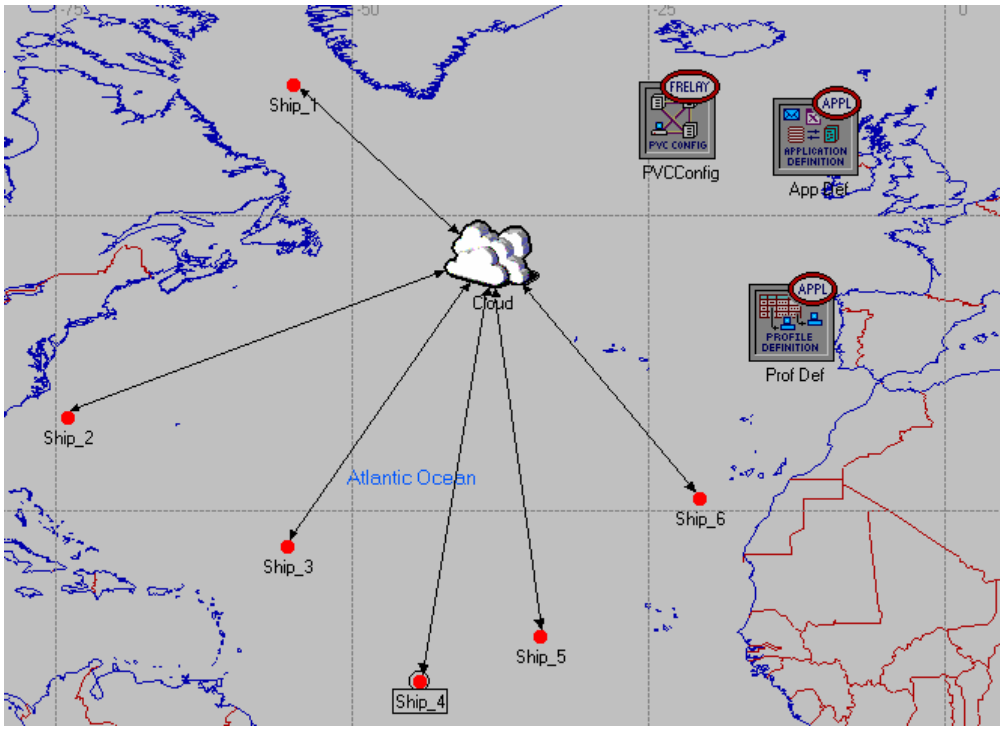

Figure 1. OPNET Model of a Battle_Group_QoS Project.

The model in Figure 1 is titled as Battle_Group_QoS. This model consists of six scenarios. The first three scenarios' links that connects each ship with the satellite (shown as a cloud in the illustration) are 10Base T in speed simulating an RF analog transmission speed with no delay imposed on the link as illustrated below in the advanced attribute section of the Battle_Group_QoS model.

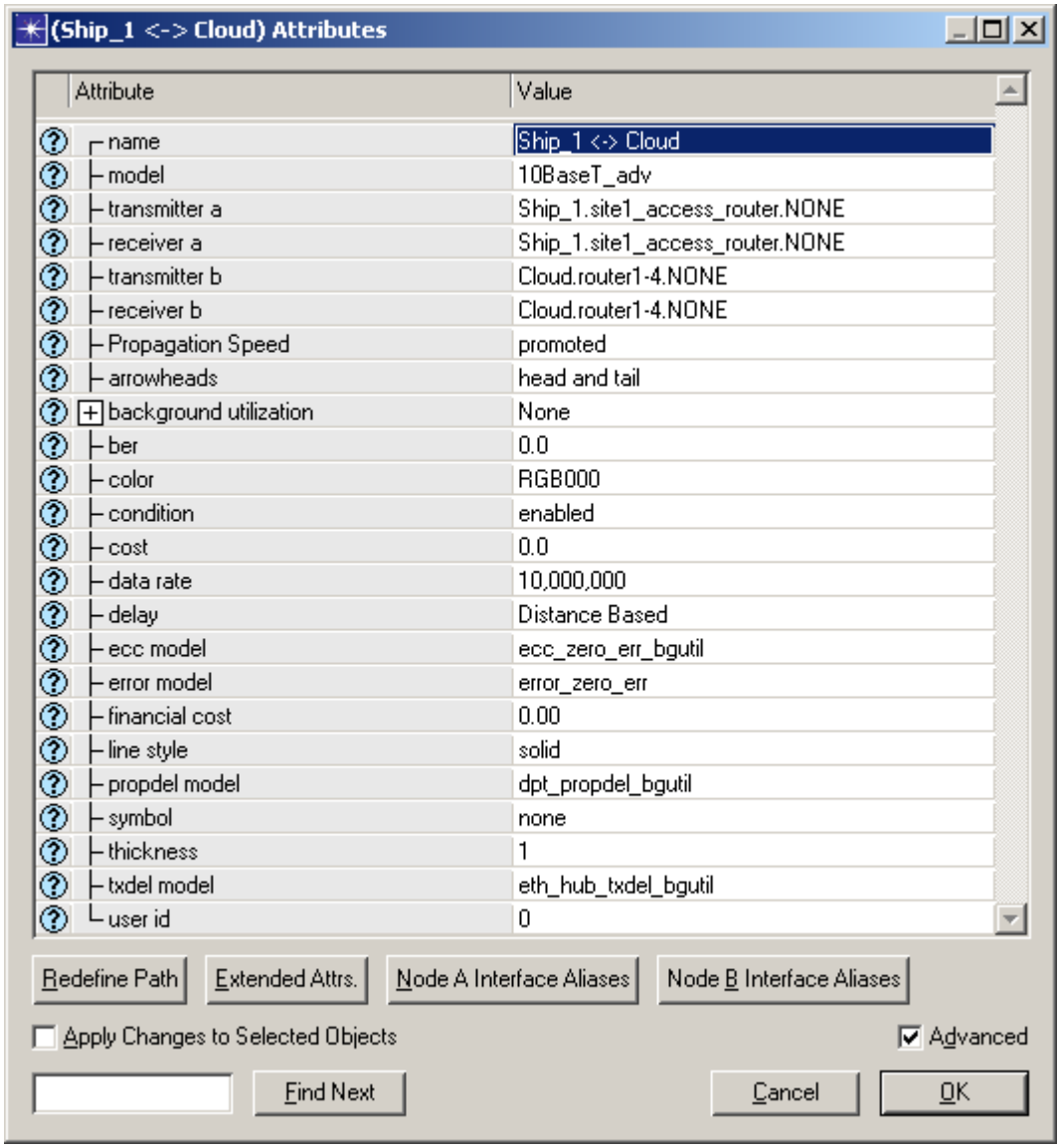

Figure 2. 10Base T Link Attribute Section.

The last three scenarios contains links that are 100Base T in speed simulating a LAN transmission speed with a 250 millisecond time delay imposed to represent delay to and from a geostationary satellite as illustrated below in the advanced attribute section of the Battle_Group_QoS model.

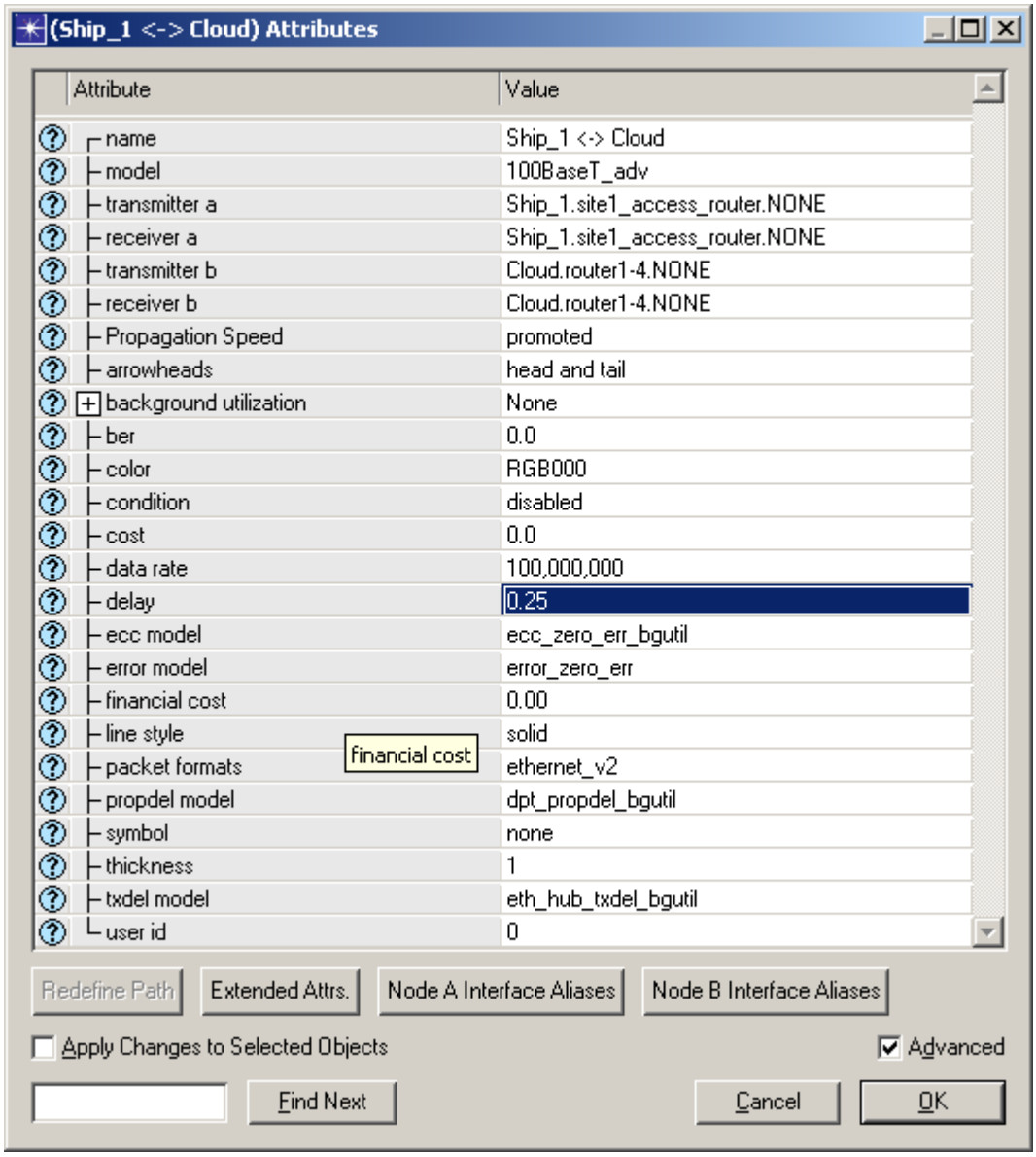

Figure 3. 100Base T Link Attribute Section.

Each ship in the model shown in Figure 1 has a LAN consisting of 18 workstations, 2 local servers, 2 LAN switches, 1 access switch and 1 access router as depicted below in Figure 2.

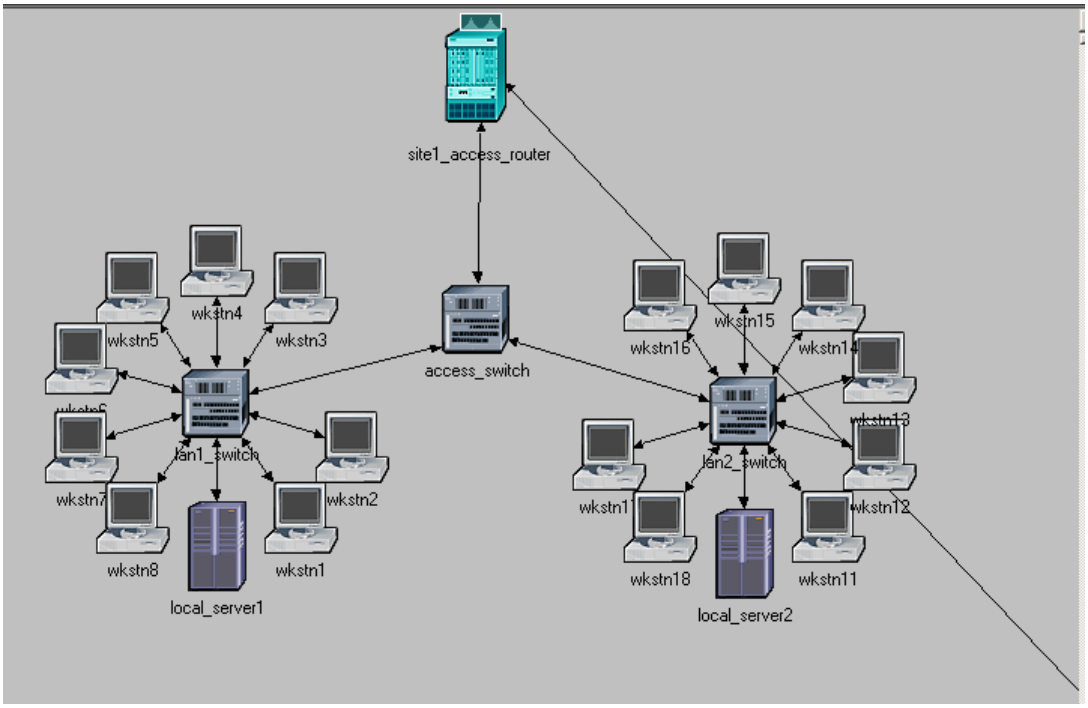

Figure 4. Shipboard SIPRNET LAN Configuration.

D. MODEL ANALYSES

The Battle_Group network model shown above in Figures 1-4 represent a typical LAN configuration of ships within a Battle Group. Consideration must be given to the following elements that are not simulated in the above model:

- There is a delay in all communications that leave the ship because of the ADNS system. ADNS selects the order that data is transmitted off the ship. The delay incurred by this process is due to as Media Access Protocol. A explicit understanding of ADNS is provided in Appendix D [Ref 7].
- There is a slight delay in analog RF voice communication because of the use of crypto for secure communications referred to as crypto synchronization.
- The interface to SIPRNET is at a NCTAMS. This is not illustrated in the model, but there is a delay incurred because all data over the SIPRNET LAN are transmitted to this point and then distributed to its destination.

Although the delay incurred may be small in measurement, the elements above should be factored in when measuring voice End-to-End delay on a network.

A major constraint on voice quality is voice ETE delay. On private network, 200 ms delay is a reasonable goal and 250 ms is a limit. [Ref 6] The network administrators

should configure the system to minimize voice delay as possible. The ITU-T recommendation G.114 summarizes three ranges of one-way delay as shown in the following table:

Table 1. Delay Specifications.

Range in Milliseconds	Description
0-150	Acceptable for most user applications.
150-400	Acceptable provided that administrators are aware of the transmission time and it's impact on the transmission quality of user applications.
Above 400	Unacceptable for general network planning purposes, however, it is recognized that in some exceptional cases this limit will be exceeded.

The results of the Battle_Group network model illustrate Voice ETE Delay and Jitter. The use of QoS controls greatly improved Voice ETE Delay as shown in the graphs in Figures 5-9.

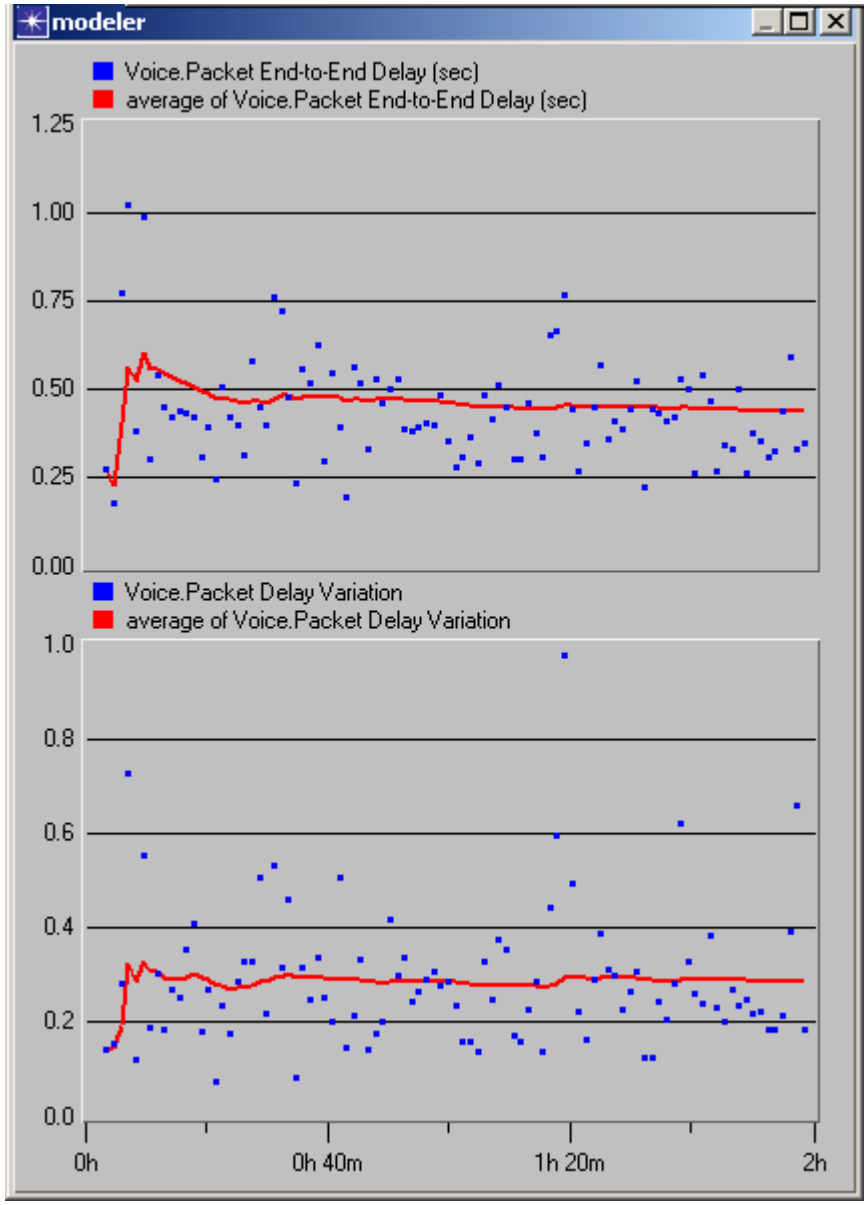

Figure 5. DES_NO_QoS 10Base T Network.

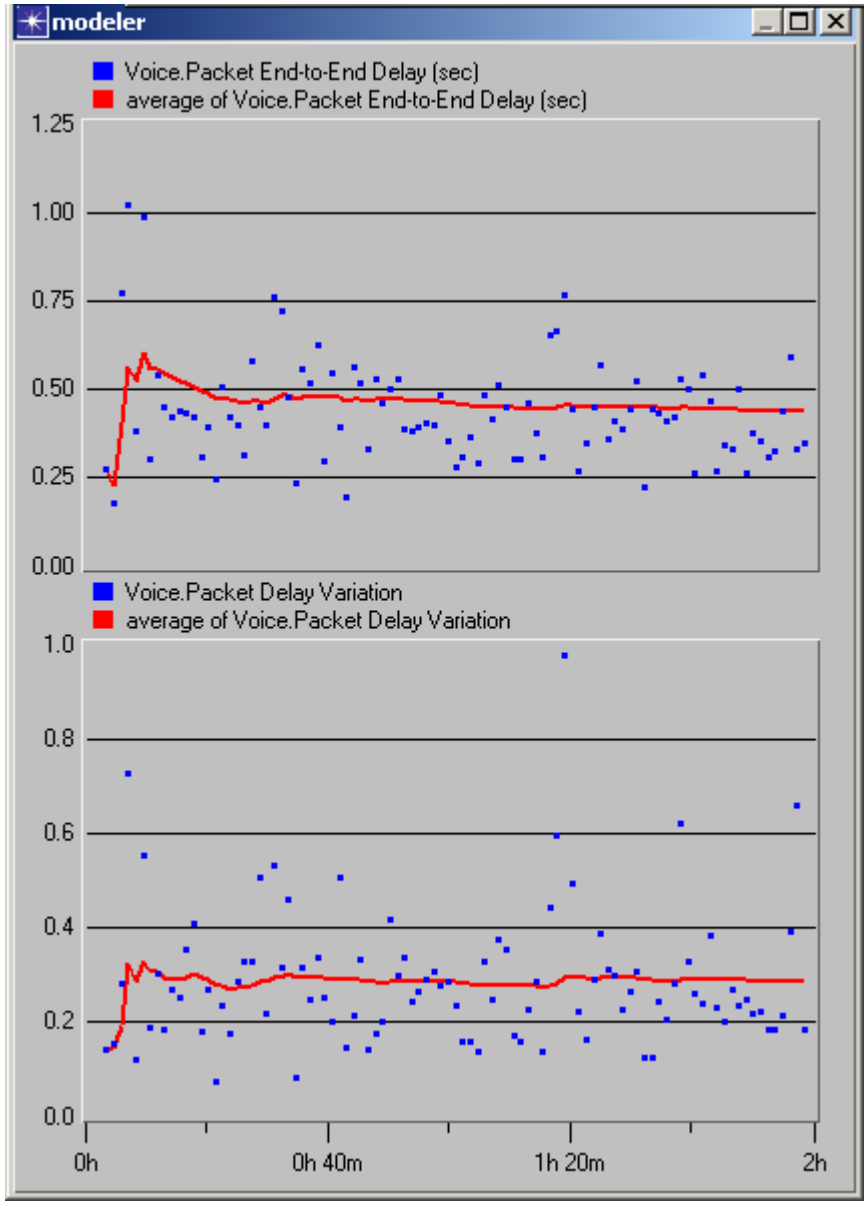

Figure 6. DES_NO_QoS 100Base T Network.

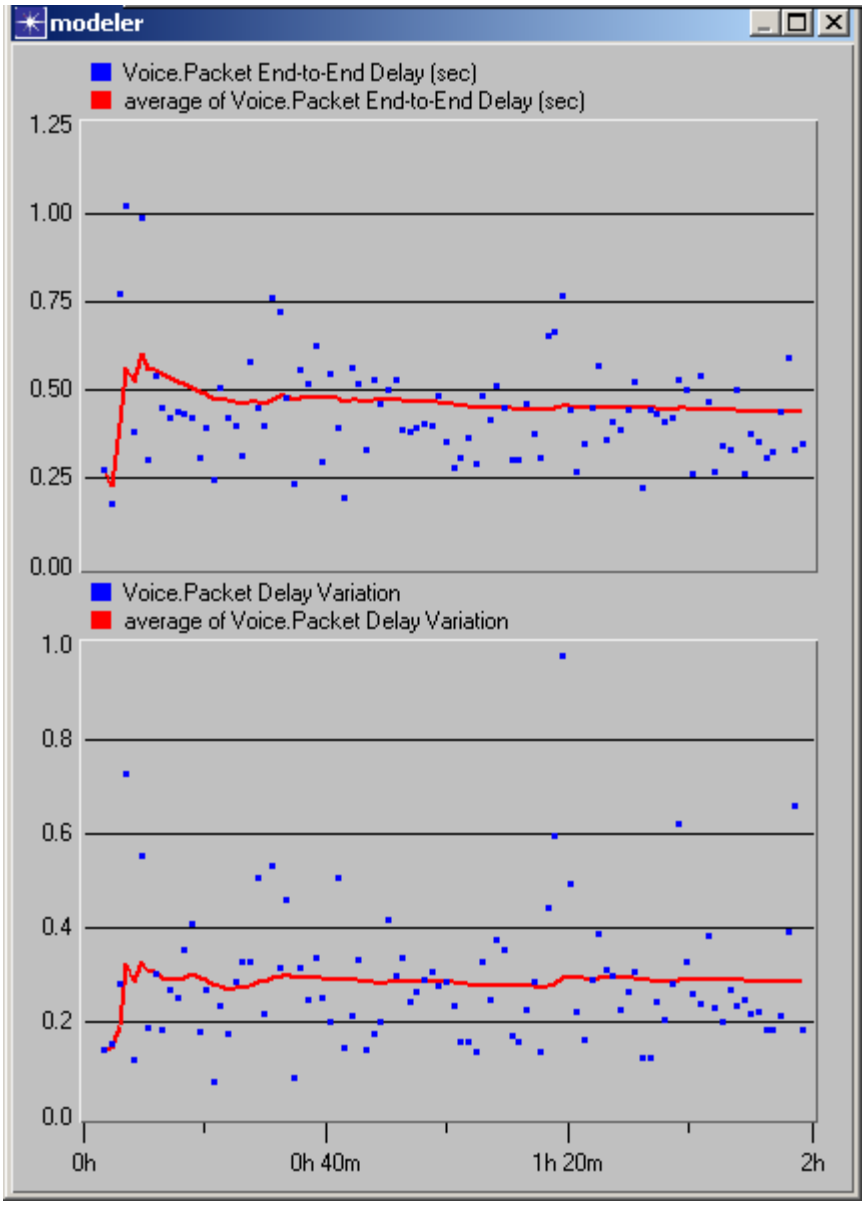

Figure 7. DES_PQ 10Base T Network.

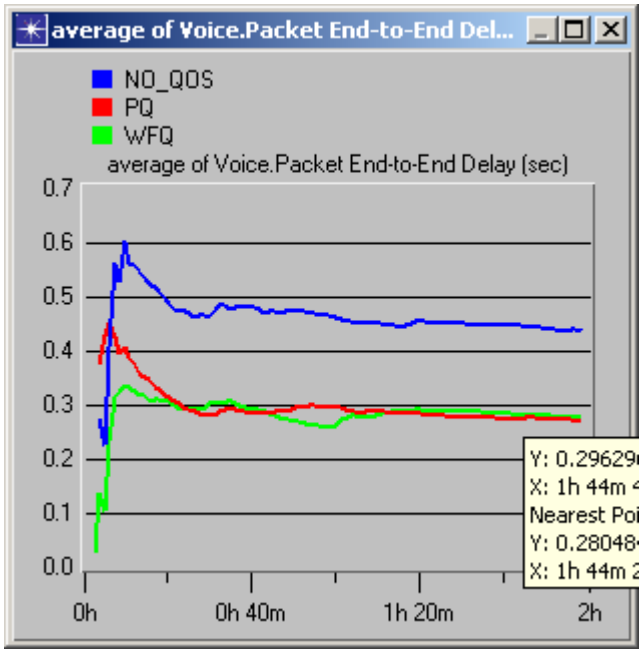

Figure 8. DES_WFQ 10Base T Network.

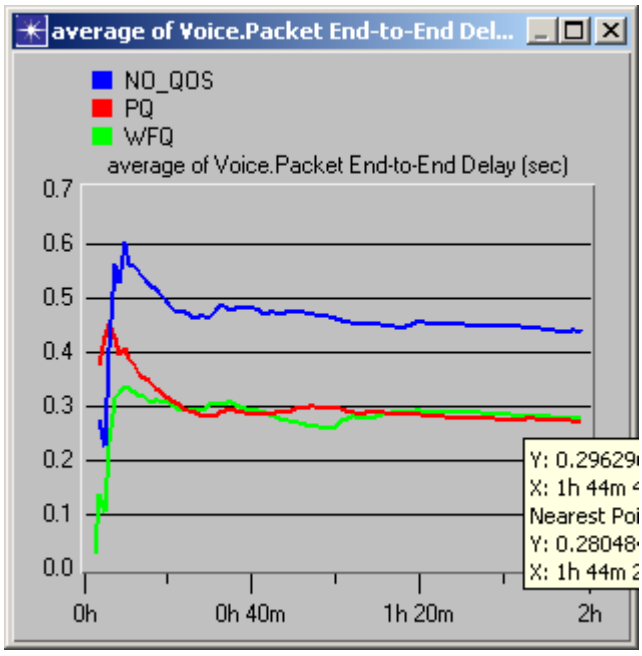

Figure 9. DES_WFQ 100Base T Network.

E. SUMMARY

The OPNET Battle_Group model evaluated voice transmissions over the network for a duration of two hours. The results shown in Figures 5-9 illustrates the voice ETE delay incurred on the network. The first two scenarios of the model were run without the implementation of priority queuing (PQ) or weighted fair queuing (WFQ) controls. The

results of voice ETE delay initially spiked up to .6 but immediately leveled off below .5 which is well within tolerance for voice transmissions. In the second two scenarios PQ was implemented and the voice ETE delay variation spiked up to 302 ms and leveled off to 172 ms which improves voice ETE delay. In the last two scenarios, voice ETE delay variation spiked up to 196 ms and leveled off to 152 ms. As shown by each scenario voice ETE delay improved with each implementation of QoS controls. The model provided above is not an exact replication of a Battle Group network but for the purposes of this research it has comparable characteristics to aid in the evaluation of latency and jitter on the network.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. RECOMMENDATION

The convergence between voice and data transmission networks is inevitable. While VoIP is still fairly new it has great potential because it is capable of supporting both data and voice. The results from the Battle_Group network model demonstrate that latency and jitter are within acceptable limits without the use of QoS controls. Although, employing QoS controls can greatly reduce latency and jitter on a network there is a trade off in service. The US Navy would benefit by adopting a phased implementation of VoIP technology. This would ensure an efficient transition into VoIP and allow for necessary training and adaptation to change.

B. FUTURE RESEARCH

Interoperability and effective communication are essential to warfighting readiness and mission accomplishment. Battle Group interoperability is a key element to executing the mission of the US Navy. Therefore, utilizing a Battle Group as a test bed platform is an effective measure of evaluating the advantages of data and voice integration using VoIP technology. To capture the additional benefits of VoIP technology, recommendations for advanced research would include evaluating costs, training, education, and effective methods of phased implementation without degrading mission readiness. Additionally, research should include evaluating a Battle Group during underway training evolutions to analyze VoIP in a live environment. This would allow for the delay considerations not illustrated in the model to be evaluated.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. QoS DATA VOICE SCENARIO

Project: QoS_Data_Voice Scenario

This project consists of two sub-projects:

1) Hybrid_Sim scenarios - using OPNET 8.0 new hybrid traffic (Conversation Pair Matrix analytically-modeled traffic, Microsimulation, and Discrete Event Simulation), a large network of over 10,000 users are modeled, implementing a VoIP rollout. Modeling techniques implemented are detailed in the documentation under modeling methodology "Simulation Methodology for the Analysis of QoS".

2) DES scenarios - all Discrete Event Simulation technique to study rollout of Voice over Frame Relay network.

For the purpose of this thesis only the DES scenarios are used to illustrate the operational benefit of implementing VoIP on a Battle Groups network.

The non-profit group Save Earth and Mankind (SEAM) has a network with several sites across the United States. SEAM's network is stretched to capacity. However, the group must cut back its budget even further. One way to do this is to use Voice over IP instead of conventional long distance service. A trial version of the service was tested out on a few sites. Although the voice traffic did not interfere too much with existing traffic, the delay on voice packets was too high (and too variable) to be useful.

SEAM's goal has two parts:

* Try to use QoS mechanisms to improve the voice performance.

* Any changes to the network must not harm existing traffic performance much.

The Scenarios:

Scenario 1: NO_QOS shows voice and data traffic.

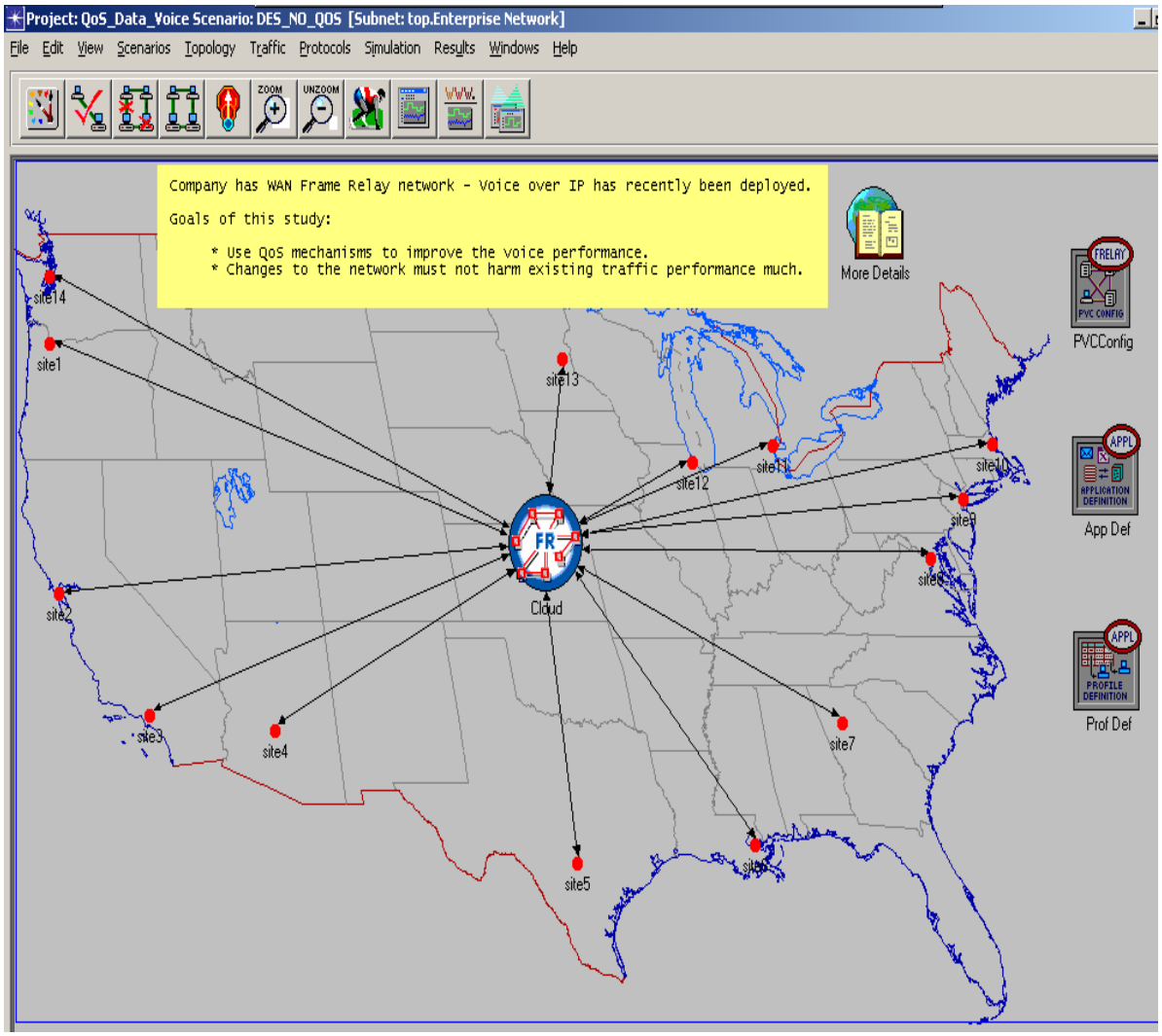

Figure 10. DES_NO_QoS.

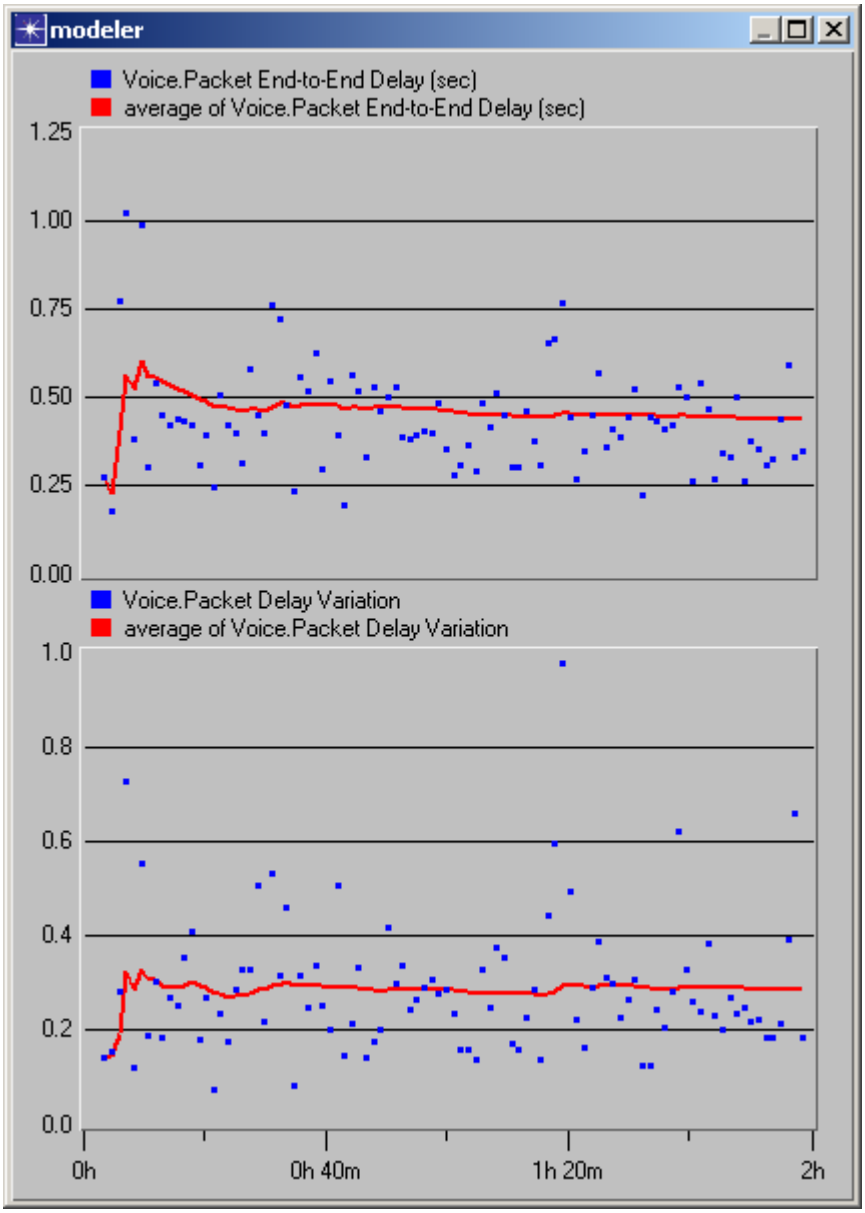

Figure 11. DES_NO_QoS Results.

Scenario 2: PQ shows the effect of priority queuing.

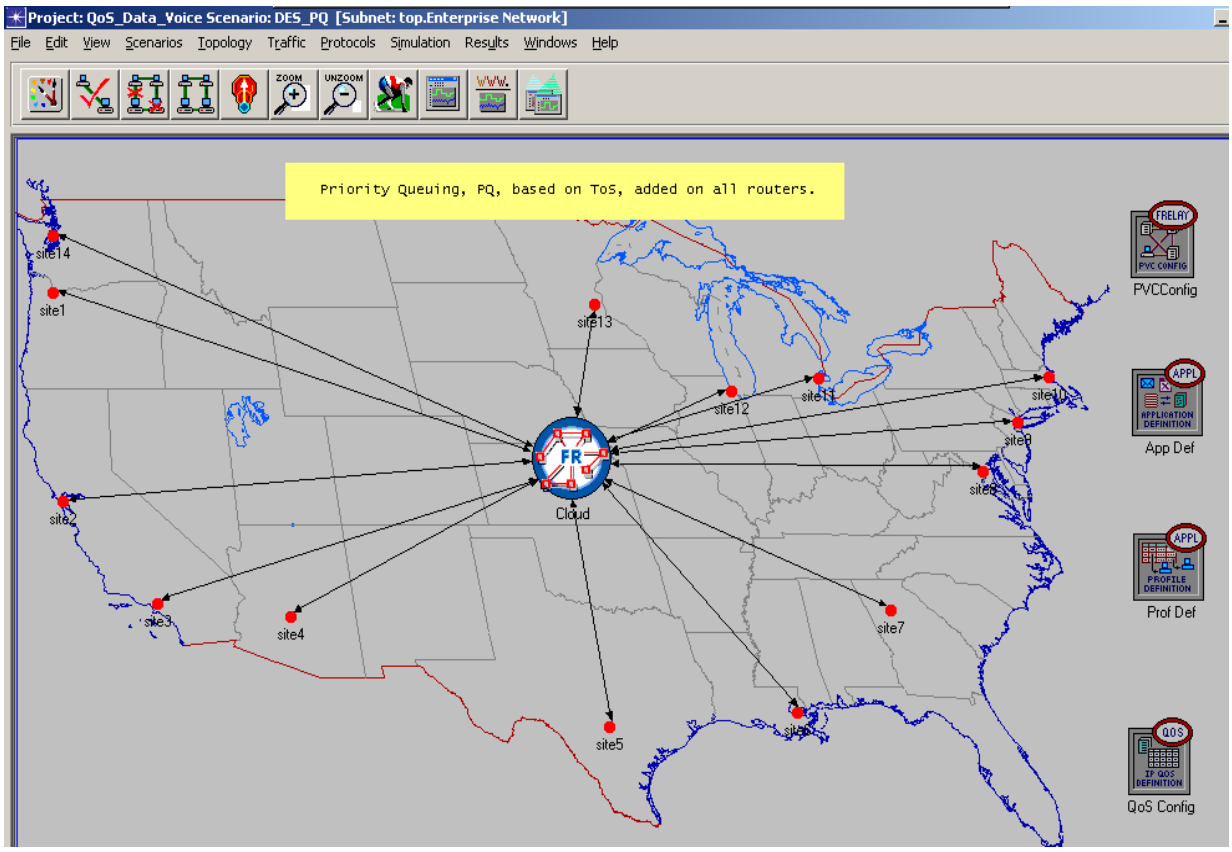

Figure 12. DES_PQ.

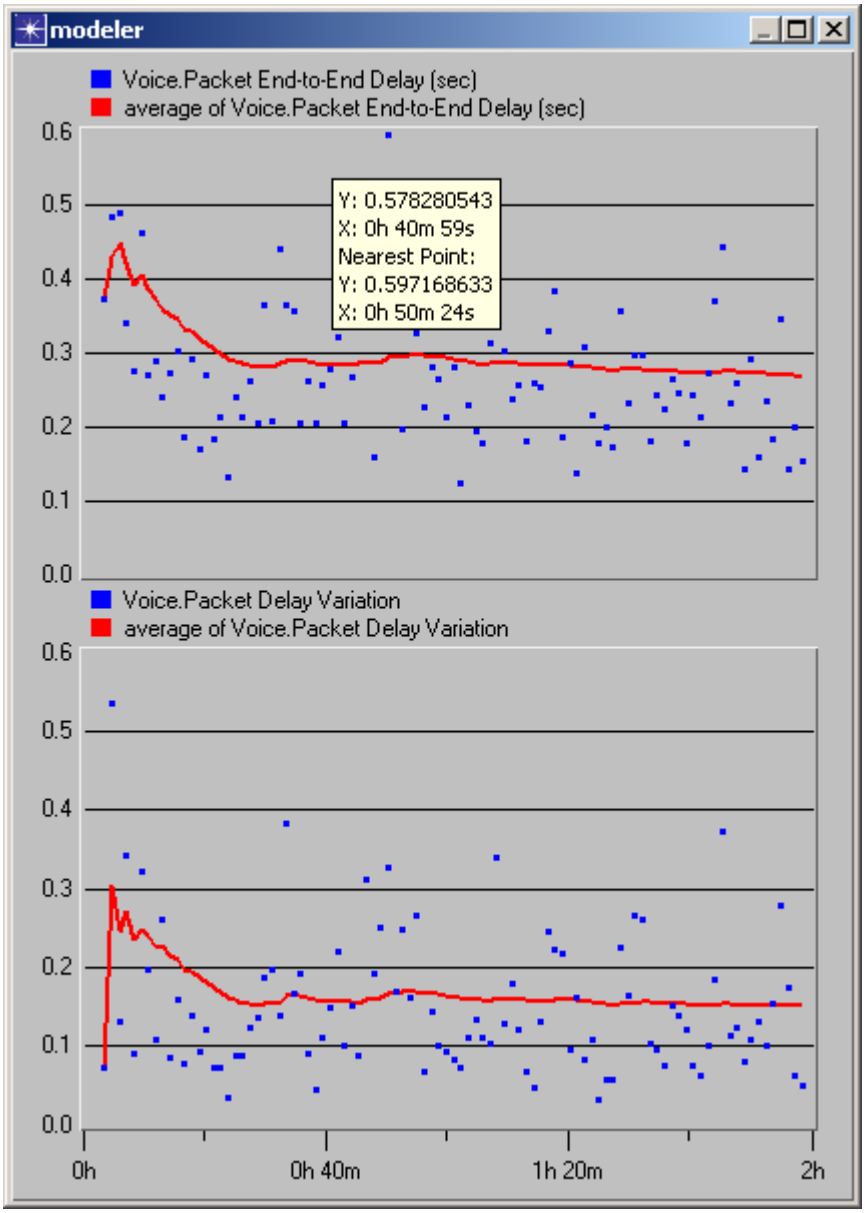

Figure 13. DES_PQ Results.

Scenario 3: WFQ show weighted fair queuing.

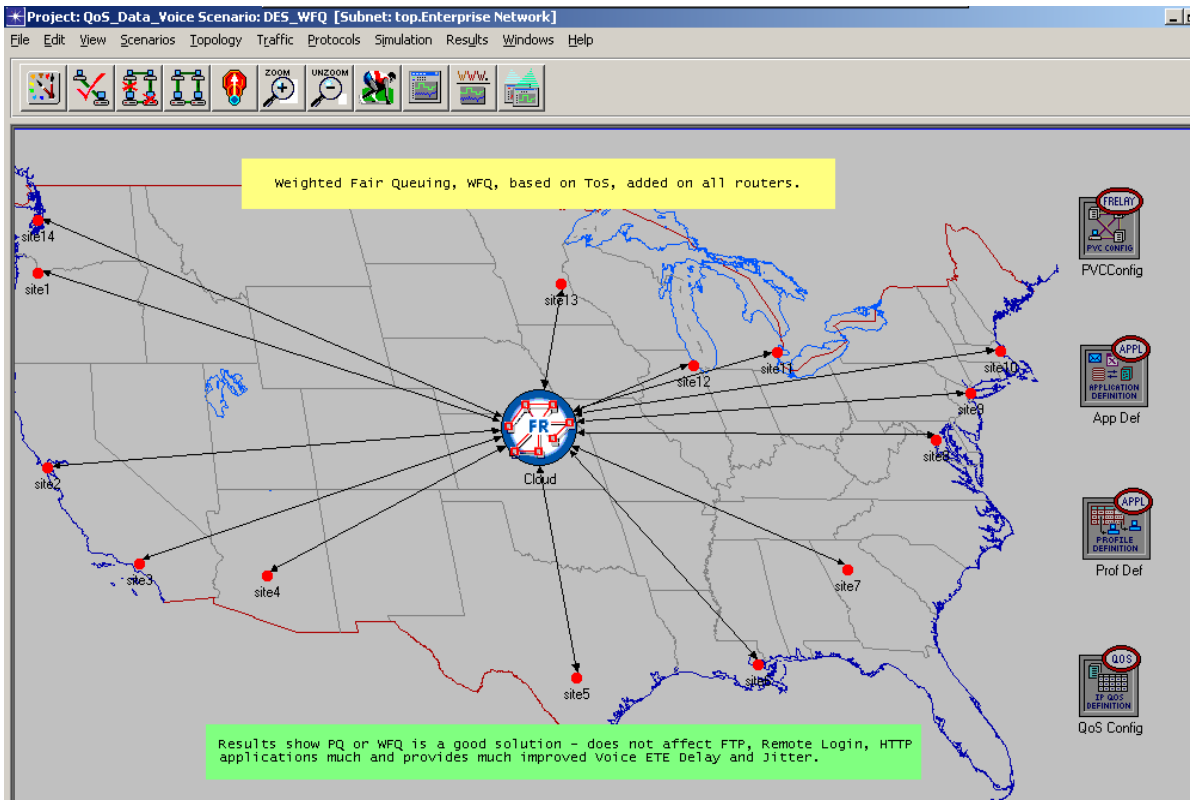

Figure 14. DES_WFQ.

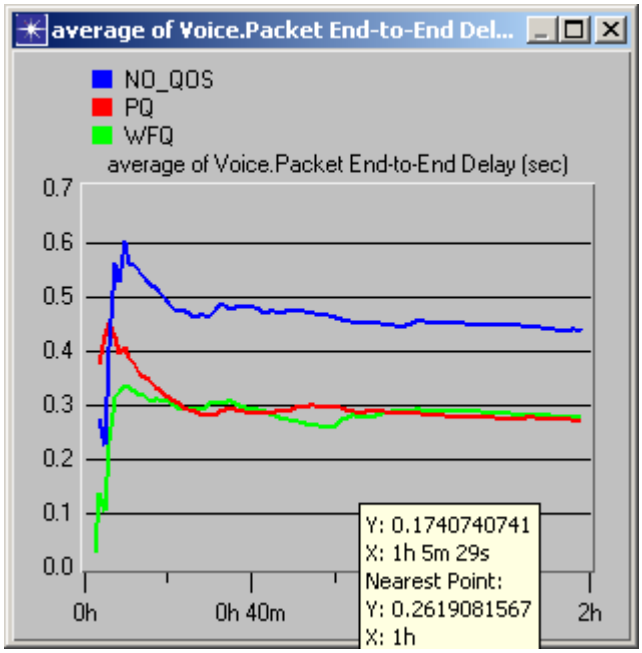

Figure 15. DES_WFQ Results.

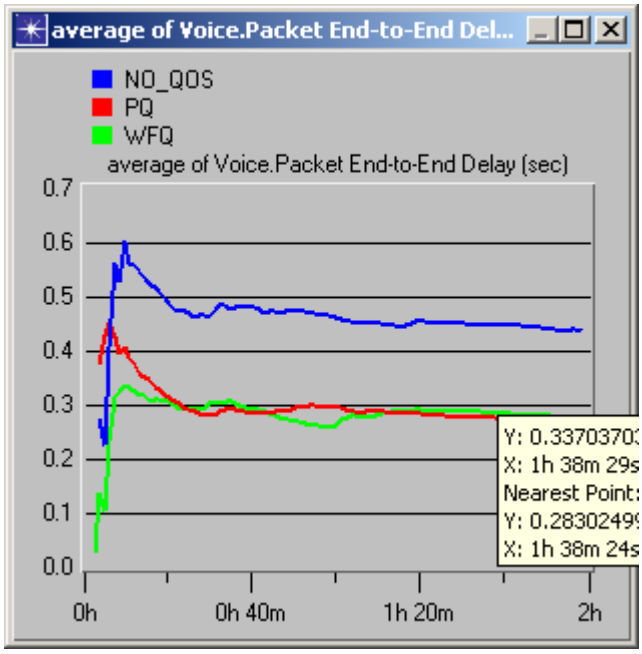

Figure 16. DES_WFQ Results.

Results show PQ or WFQ is a good solution - does not affect FTP, Remote Login, and HTTP applications much and provides much improved Voice ETE Delay and Jitter.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. QOS ATTRIBUTE CONFIGURATION OBJECT

The QoS Attribute Configuration object defines profiles for the following technologies:

- CAR
- FIFO
- WFQ
- Custom Queuing
- Priority Queuing

Each queuing-based profile (e.g., FIFO, WFQ, PQ, CQ) contains a table in which each row represents one queue. Each queue has many parameters such as queue size, classification scheme, RED parameters, etc.

Note that the classification scheme can also be configured to contain many different criteria by increasing the number of rows. Some examples of setting queue priorities are:

- Weight for WFQ profile. Higher priority is assigned to the queue with a higher weight.
- Byte count for Custom Queuing profile. More traffic is served from the queue with a higher byte count.
- Priority label for Priority Queuing. Higher priority is assigned to the queue with a higher priority label.

The CAR profile defines a set of classes of service (COS). Each row represents a COS for which CAR policies has been defined.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. WHEN/WHY SHOULD I USE QoS IN MY NETWORK?

Queuing schemes provide predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved packet loss characteristics.

The basic idea is to pre-allocate resources (e.g., processor and buffer space) for sensitive data. Each of the following schemes require customized configuration of output interface queues.

- Priority Queuing (PQ) assures that during congestion the highest priority data does not get delayed by lower priority traffic. However, lower priority traffic can experience significant delays.

(PQ is designed for environments that focus on mission critical data, excluding or delaying less critical traffic during periods of congestion.)

- Custom Queuing (CQ) assigns a certain percentage of the bandwidth to each queue to assure predictable throughput for other queues. It is designed for environments that need to guarantee a minimal level of service to all traffic.

- Weighted Fair Queuing (WFQ) allocates a percentage of the output bandwidth equal to the relative weight of each traffic class during periods of congestion.

RED is a dropping mechanism based upon the premise that adaptive flows such as TCP will back off and retransmit if they detect congestion.

By monitoring the average queue depth in the router and by dropping packets, RED aims to prevent the ramp up of too many TCP sources at once and minimize the effect of that congestion.

CAR is a traffic regulation mechanism, which defines a traffic contract in routed networks. CAR can classify and set policies for handling traffic that exceeds a certain bandwidth allocation. CAR can be also used to set IP precedence based on application, incoming interface and TOS. It allows considerable flexibility for precedence assignment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. ADNS [REF 7]

ADNS uses three open standard Internet protocols to accomplish its routing functions: Open Shortest Path First (OSPF), Multicast OSPF (MOSPF) and Border Gateway Protocol Version 4 (BGP4).

A. DEFINITIONS

The following general definitions are applicable to all three protocols.

- Autonomous System (AS) - "A group of routers exchanging routing information via a common routing protocol (Moy, 1997).
- AS Boundary Router (ASBR) - A router which links an AS to other ASs. (Moy, 1997).
- Interior Gateway Protocol (IGP) - "The routing protocol spoken by the routers belonging to an AS" (Moy, 1997). Although different ASs may be using different IGPs, each AS only uses one. OSPF is an IGP. All ADNS ASs use OSPF.
- Area - A group of networks whose topology is hidden from the rest of the AS. "An area is a generalization of an IP subnetted network" (Moy, 1997). In ADNS each ADNS installation (ship or shore site) will usually be considered an area (Johnson, 1997).
- Backbone - The common area through which areas are attached (Johnson, 1997).
- Area Border Router (ABR) - A router attached to more than one area (Moy, 1997). In ADNS installations it is the area router attached to the backbone (Johnson, 1997).

- Exterior Gateway Protocol (EGP) - A routing protocol used to communicate between ASs. BGP4 is an EGP. Routing between ASs in ADNS is done via BGP4.

B. INTERNAL ROUTING

1. OSPF

a. General

OSPF is a dynamic routing protocol used to communicate between routers in an AS. OSPF is connectionless, operating at the network layer of the OSI model. Each IP datagram is independently routed to its destination based on the destination IP address in the packet header. The full specification for OSPF Version 2 can be found in (Moy, 1997). Except where specific reference is made to the ADNS implementation of OSPF, this description is a consolidation of relevant sections of that RFC.

The dynamic feature of OSPF means that each router maintains a frequently updated link-state database containing information about all other routers in the AS. This information is used to create a table of paths to every other router and network in the AS. Each path has an associated cost. The route by which each packet is sent is the lowest cost path chosen by the router. Costs are calculated based on a dimensionless metric value assigned to each path.

OSPF allows for the subdivision of an AS into areas to reduce the communications required to maintain the status of the network. When areas are established the topology within an area is hidden from the rest of the AS and the topology of the rest of the AS is hidden from that area. In an AS that has not been divided into

areas each router has an identical link state database. When areas are used only those routers connected to the same area have identical databases.

It is the job of the ABR to represent the consolidated route structure of the backbone into its area and to provide the rest of the ABRs in the AS with the information necessary to route information into its area. To perform this function the ABR runs a copy of the algorithm for each area to which it is attached.

When areas are used the backbone is also considered an area. It contains all ABRs in the AS. "The backbone must be contiguous. However it need not be physically contiguous; backbone connectivity can be established/maintained through the establishment of virtual links" (Moy, 1997). A virtual link is established by configuring one area to act as a relay for another area. For example, area A is connected to both the backbone and area B. Area B is only connected to area A. Area A can be configured to act as a virtual link to connect B to the backbone. The route to B is advertised through A.

b. The Link State Database and Routing Table

Each router on the network maintains a link state database that includes the cost for each connection in the network. Since the costs associated with a given connection are direction sensitive the database contains both a "to" and "from" entry for each connected network or router. For example, if two routers, R1 and R2, are connected there will be entries for R1 to R2 and R2 to R1. The cost for each may be different, depending on the metric values assigned.

The router calculates a routing table of shortest paths to each destination from the link-state database. This table has three columns: destination, next hop and distance. There is a line item for each network. Although the algorithm calculates the

entire path, only the next router (next hop) is entered in the routing table. Distance is the total cost to the destination network as calculated from a particular router. Since the shortest route to any destination depends on the starting point, the routing table will be different for each router.

c. Link State Advertisements

The Link State Database is built from the information provided in Link State Advertisements (LSAs) received by the router. LSAs describe the current state of the connections within a network as seen by a given router at a specific time. There are five different types of LSAs:

- Type 1: Router-LSA. Describe the links a router has to an attached area. Included in this description is the metric value assigned to each link.
- Type 2: Network-LSA. Sent by the DR on Broadcast and NBMA networks this LSA lists all routers connected to the network.
- Types 3 and 4: Summary-LSA. There are two types of Summary-LSA. Sent by an ABR this LSA describes a route to a destination outside of that area but still inside the AS. One type gives routes to ASBRs. The other type gives routes to networks. Included in the Summary-LSA is the metric value for the entire route to the destination.
- Type 5: AS-external-LSA. Sent by an ASBR this LSA describes a route to a destination in another AS. This LSA also contains a metric value describing the cost of the route.

d. Routing Protocol Types

To establish and maintain the status of the network information in various

forms must be passed among routers in an AS. To accomplish this OPSF uses five different protocol packet types: Hello, Database Description, Link State Request, Link State Update and Link State Ack. With the exception of Hello packets these packets are sent only over adjacencies. Among the information found in each packet is:

- Router ID. Uniquely identifies the originating router.
- Area ID. Identifies the area to which the originating router is connected and which is the source of the packet. Packets are associated with areas vice routers since routers can interface with more than one area but the information in a packet describes relationships with respect to an area.
- Authentication. Each packet is authenticated, thus only trusted routers may participate in a network.

The Hello packet is used to find and maintain neighboring routers. It is also used in the Designated Router (DR) election process. Among the additional information included in a Hello packet is:

- HelloInterval. Interval at which Hello packets will be generated. This value must be the same for every router on the network.
- RouterDeadInterval. Elapsed time from receipt of last Hello packet before a router is declared down. This value must be the same for every router on the network.
- Designated Router. IP address of the DR. If no DR has been elected this field is set to 0.0.0.0.
- Backup Designated Router (BDR). IP address of the BDR.

- Neighbor. Router ID of any router whose Hello packets have been received by the originating router within the last RouterDeadInterval seconds. This field is repeated as necessary, once for each neighbor.

The Database Description packet is used between two routers when adjacency is being established. Information in the packet includes:

- DD Sequence Number. Each packet is sequentially number to ensure continuity between the two routers exchanging data.
- LSA Header. The header information (vice the fully database entry) for each LSA in the database. Due to packet size limitations each packet can only hold a finite number of LSA headers. Consequently to fully describe a database will usually require multiple Database Description packets.

Generated in response to a Database Description packet, the Link State Request packet is used to request missing parts of a link state database. The Link state request identifies the LSA for which an update is needed. Each Link State Request can request multiple LSAs. Similar to a Database Description packet the packet can contain multiple LSA header fields.

Link State Update packets are sent in response to Link State Requests or when the status of a router changes. In addition to the LSA header the packet also contains the full LSA. Each packet can contain multiple LSAs and they can have originated from different routers.

Link State Acknowledgement packets are sent to acknowledge receipt of Link State Updates. The body of the Link State Acknowledgement packet lists the LSA headers for which receipt is being acknowledged.

e. Establishing a Connection

To support the dynamic nature of the protocol OSPF routers must communicate often to pass information regarding the status of the network. The functions performed by a router when it is first brought into the network can be divided into a sequence of four steps; discovering neighbors, verifying two-way communications, electing a designated router (for broadcast and non-broadcast multi-access (NBMA) networks) and, if appropriate, establishing adjacency.

(1) Discovering Neighbors and Verifying Two-way Communications. To ensure delivery of data each router in the AS must have an accurate picture of the current state of the network. The first step in forming this picture is to determine what other routers are available. This process of neighbor discovery is accomplished using the Hello Protocol. Each router will upon startup and periodically thereafter send Hello packets to other routers in the AS. The Hello packet allows each router to advertise its status to other routers.

The hello packet sent by a given router contains an entry for every other router for which it has received a current hello packet. As the newly started router receives Hello packets from other routers it updates its own Hello packets. At the same time other routers in the network are updating their packets by adding the new router. Two-way communications are verified when a router see itself listed in the Hello packet of another router.

(2) Electing the Designated Router (DR) and Establishing Adjacency. On networks with multiple routers (broadcast and NBMA networks) maintaining an updated network status on all participating routers can contribute a

significant amount to the traffic on the network. To help control the amount of traffic on these types of networks the OSPF protocol provides for the electing of a designated router and the establishing of adjacencies. To minimize traffic only adjacent routers exchange routing information updates.

Each router is assigned a router priority. That priority is included as a data field in the Hello packet. The designated router is usually the router with the highest router priority. When the new router enters the network it looks for a DR. This discovery process is done by the examination of incoming Hello packets. The hello packet generated by each router indicates which routers it thinks are the DR and Backup DR (BDR). If a DR has not been elected and the new router has the highest priority in the network then it will become the designated router. If there is already a DR then the new router will accept the existing DR, even if the new router has a higher priority. Although it makes it harder to identify which is the DR, this method creates less disruption for the network since shifting of DRs requires updating the databases on all routers in the network. This disruption could cause delays in routing of data on the network while the router databases are being updated.

In addition to the DR there may also be a BDR. This is to avoid network disruption when the DR fails. Since each router already knows the identity of the DR and BDR the shift to the BDR on a loss of the DR will not require excessive network communications to reestablish the state of the network. To minimize the number of shifts the most dependable router in the network should have the highest priority so that it will eventually become the DR.

Once the DR and BDR have been elected the process of forming

adjacencies begins. Not all routers become adjacent. Routers only become adjacent to the DR and BDR. To become adjacent means that the link state databases of the two routers are synchronized. To synchronize databases the routers must exchange database status information. This is done via Database Description packets. The two routers establish a master-slave relationship for this Database Exchange Process. The master sends the status of its database via Database Description packets. The slave receives these packets and acknowledges receipt by sending a Database Description packet with the same DD sequence number and its version of the LSA header information back to the master. Each router then compares the LSA information to its own database. If either router has data that is older than the other router's it requests an update via a Link State Request. When the Database Exchange Process is complete both databases are identical and are considered synchronized and the routers are considered to be adjacent.

f. Network Maintenance

To ease the communication overhead associated with maintaining the network several of the OSPF protocol packet types can be sent via IP multicast. There are two IP multicast addresses used in OSPF, AllSPFRouters and AllDRouters. All routers running OSPF should be configured to receive packets addressed to AllSPFRouters. Each router sends Hello packets using AllSPFRouters. The DR will also use AllSPFRouters when sending Link State Update messages to all adjacent routers. Adjacent routers use AllDRouters to send Link State Updates to the DR and BDR.

It is important to note that since it is only one hop from the DR or BDR to any adjacent router then all of the packets that travel only over adjacencies travel only one hop. Since Hello packets are sent to immediate neighbors this means that no OSPF

packet is required to travel farther than one hop from its source. The only exception is for virtual links that may need to forward packets to their ultimate destination.

Maintaining the status of the network current requires the periodic passing of all of the different types of messages at varying intervals. Hello packets are sent at an operator selectable interval set by the HelloInterval setting in the Hello packet. The value chosen should be significantly less than the RouterDeadInterval to avoid unnecessarily terminating connections. Database Description packets are retransmitted by the DR at fixed 30 minute intervals. Link State Requests, Updates and Acknowledgements are sent as needed in response to changes in the network topology.

g. Packet Routing

Routing of packets is done in three steps. Intra-area routing through the area of the originating network, inter-area routing across the backbone area and intra-area routing through the area containing the destination network. The algorithm finds the combined set of paths with the smallest cost. The router consults the routing table for the destination address of each packet and forwards it to the Next Hop router listed in the table. The process is repeated at each router until the destination is reached.

2. MOSPF

a. General

Multicast OSPF is an enhancement to the OSPF routing protocol that allows for the multicasting of IP datagrams (Moy, 1994). The full specification for MOSPF can be found in (Moy, 1994). Because it relies heavily on the existing OSPF structure this discussion of MOSPF serves to highlight the important differences between the two protocols. This description is a consolidation of relevant sections of the MOSPF

RFC.

b. Characteristics of MOSPF

MOSPF adds one additional LSA to those already used by OSPF. The group-membership-LSA serves to identify multicast group members in the existing OSPF database. Much like OSPF the multicast extension calculates a shortest path tree for transmitting datagrams, using the same metric values as OSPF. However, unlike OSPF, this tree is calculated on demand, when the first datagram in the transmission is received.

MOSPF also differs from OSPF in that in OSPF IP datagrams are routed based on destination IP address only, in MOSPF datagrams are routed based on both source and destination addresses. When routing datagrams MOSPF will take advantage of any common paths among the destination addressees. The datagram will not be replicated until the paths diverge.

MOSPF does not allow for equal cost multi-path routing. Only one path will be selected for each destination IP address. Due to the division of an AS into areas each router does not have a complete picture of the AS since only summary information is advertised across area boundaries. As a result, the routing of datagrams may be less efficient due to the hiding of paths performed by the ABRs.

C. EXTERNAL ROUTING

1. BGP4

a. General

BGP4 is a routing protocol for use between autonomous systems. However, unlike OSPF, BGP4 is not a dynamic protocol. Routing decisions are based on policy. Routes are predetermined and remain relatively stable. BGP4 must be run over a reliable transport protocol. Since TCP is used on most routers and hosts it is used as BGP4s transport protocol. The specification for BGP4 can be found in (Rekhter and Li, 1995). Specifics on implementation of BGP4 in the Internet can be found in (Rekhter and Gross, 1995). Except where specific reference is made to the ADNS implementation of OSPF, this description is a consolidation of relevant sections of these RFCs. The discussion of determining route preferences is consolidated from (Rekhter and Gross, 1995) all other portions are from (Rekhter and Li, 1995).

b. BGP4 Message Types

There are four different message types used by this protocol to communicate between BGP4 hosts.

- Open. This is the first message sent by both ends of a connection. In addition to fields that identify the sending router and its associated AS this message also contains a Hold Time field. Hold Time is the number of seconds allowed between receipt of Update or Keep Alive messages before a link will be considered down.
- Update. This message type is used to transfer the routing table information

between two routers. The message format allows for the transfer of a single feasible route to a destination or to remove unfeasible routes. One message can be constructed to perform both functions.

- Notification. Notifications are sent to indicate an error condition has occurred. The connection along which the message is sent is closed immediately after receipt of the Notification. A Notification will be generated as a result of errors in message content or as a result of the hold timer expiring.
- Keep Alive. A Keep Alive message is used to maintain the open status of a connection. One is sent in response to a valid Open message. When no other messages (i.e., Updates) are being sent a Keep Alive will be generated to maintain the link active. Keep Alive messages are normally sent at about one third of the Hold Time Interval.

c. Operation

The first step in the routing process is the establishment of a TCP connection between the source and destination. Next the entire BGP routing table is sent across the link. Because BGP4 does not require periodic refreshing of the routing table the host must maintain the received table for the duration of the connection. Updates to the table are generated when changes are made.

Once the routing table has been sent the connection is maintained open through the use of periodic Keep Alive messages or Updates. Data is passed via the advertised route to its destination.

d. Routing Decision Process

Each router receives route information from other BGP4 routers via

Updates. This routing information is maintained in a database in the router. The router then applies a set of decision rules to this data to determine its preferred route to a particular destination. The decision process occurs in three phases. The ultimate output of the decision process is a table of routes that are to be advertised to other BGP4 routers.

Phase one involves determining the degree of preference associated with routes received from other BGP4 routers. Upon receipt of an Update message the router will invoke the preference policy implemented in the router. The policy is determined locally for each router and is implemented in the form of configuration information in the router. In general this preference decision can be based on path information or other policy or a combination of both. Path information can include such things as AS count, which is the number of systems that must be traversed to reach the destination. Policy can be used to avoid certain links because of known problems such as reliability or stability. If there are multiple BGP4 routers in an AS they will all invoke the same set of policies. Based on these policies they must internally agree on which router will be advertised to neighboring BGP4 routers as the gateway to that AS.

Phase two evaluates routes to select the preferred route to be advertised to other systems. Once phase one is completed every route to a specific destination is compared and the route with the highest preference is selected. If there is only one route to a particular destination no decision is required and that route is then selected. The result of this phase is a table of containing one preferred route to each reachable destination.

Phase three involves the passing of the results of this process to other BGP4 routers. This is accomplished through the use of Update messages.

LIST OF REFERENCES

1. Telecommunications: Glossary of Telecommunication Terms, General Services Administration Information Technology Service, [http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm], 20 October 2002.

2. VoIP, [http://www.protocols.com/index.htm], 24 April 2003.

3. [http://www.cisco.com/warp/public/788/AVVID/csaaipm.html#qosissues], 24 April 2003.

4. The Carrier Strike Group, [http://www.chinfo.navy.mil/navpalib/ships/carriers-/powerhouse/cvbg.html], 24 April 2003.

5. FAS, Radio Communications System, [http://www.fas.org/man/dod-101/sys/ship/weaps/radio.htm], 24 April 2003.

6. Cisco System, "Understanding Delay in Packet Voice Networks", White Paper, [http://www.cisco.com], 24 April 2003.

7. Sullivan, James A., "Management of Autonomous Systems in the Navy's Automated Digital Network System (ADNS), September 1997.

8. Bart, R., et al., "A Comparison of Voice Over IP (VoIP), Asynchronous Transfer Mode (ATM) and Time Domain Multiplexing (TDM) Baseband," (Space and Naval Warfare Systems Command, San Diego, California, March 2002).

9. Black, Uyless, Voice Over IP, (Prentice Hall, Upper Saddle River, New Jersey, 2000).

10. ITU-T Recommendation Q.310, Definition and Function of Signals, (Geneva, 1988).

11. Caputo, Robert, Cisco Packetized Voice & Data Integrated, (McGraw-Hill, San Francisco, California 2000).

12. ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems, (Geneva 2000).

13. MGCP Media Gateway Control Protocol, Technical White Paper, (Integral Access, Chelmsford, Massachusetts, 2001).

14. Walker, John Q., A Handbook for Successful VoIP Deployment: Network Testing, QoS, and More, (NetIQ Corporation, 2001).

15. Yocom, Betsy, et al., "VoIP Makes Strides," Network World, (January 2002).

16. Yocom, Betsy, et al., "Vendors Pass VoIP Interop Hurdle," Network World, (March 2001: 45-47).

17. "Enterprise Class IP Solutions (ECLIPS)," Avaya IP Call Processing White Paper, (November 2000).

18. Naval Integrated Networks, PMW 158, Presentation, "Automated Digital Network System," (Space and Naval Warfare Systems Command, San Diego, California, April 2000).

19. ITU Recommendation I.255.3, Multi-Level Precedence and Preemption Service (MLPP), (Geneva, 1990).

20. Polk, James M., Internet Engineering Task Force Internet Draft, An Architecture for Multi-Level Precedence and Preemption over IP, [http://www.ietf.org/internet-drafts/draft-polk-mlpp-over-ip-01.txt], November 2001.

21. "Designing the IP Telephony Network," [http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm#80278], May 2002.

22. "VoIP over PPP Links with Quality of Service (LLQ / IP RTP Priority, LFI, cRTP)," [http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.html], August 2002.

23. "Cisco Catalyst 2950-24 and 2950-12 Fast Ethernet Switches," http://www.cisco.com/univercd/cc/td/doc/pcat/ca2950fe.htm - xtocid9], August 2002.

24. "Customer Profile – IP Telephony Settles the SCORE," [http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/score_cp.htm], June 2001.

25. "Cisco IP Telephony Network Guide, Cisco CallManager Clusters", [http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/], August 2002.

26. "OPNET Modeler 9.0".

INITIAL DISTRIBUTION LIST

1. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

2. Defense Technical Information Center
   Fort Belvoir, Virginia

3. Department of the Navy
   Office of the Chief of Naval Operations (N6109)
   Washington, DC

4. Naval Network Warfare Command (N61)
   Norfolk, Virginia

5. Fleet Information Warfare Center
   NAB Little Creek
   Norfolk, Virginia

6. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

7. LCDR Steven J. Iatrou
   Naval Postgraduate School
   Monterey, California

8. LT Rosemary Lewis
   Naval Postgraduate School
   Monterey, California

9. LT JaJa Marshal
   Naval Postgraduate School
   Monterey, California